4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,033	07/24/2003	John Gavan	COS94041C1	3709

25537 7590 06/30/2006

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER
AGWUMEZIE, CHARLES C

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/627,033	**Applicant(s)** GAVAN ET AL.	
	Examiner Charlie C. Agwumezie	**Art Unit** 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *03/14/05; 07/24/03*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6, and 7-27, are rejected under 35 U.S.C. 102(b) as being anticipated by Phelps U.S. Patent No. 5,602,906.

1. As per **claim 1**, Phelps discloses a method for detecting fraud in a telecommunications system, the telecommunications system generating network event records each network event record being generated in response to an event in the telecommunication system, the method comprising the steps of:

(1) performing at least one fraud detection test on the network event records (col. 1, line 1-15, 30-39);

(2) generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test (fig. 2; col. 2, lines 40-67);

(3) correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud (col. 2, lines 30-40; col. 2, line 63-col. 3, line 5; col. 4, lines 40-50); and

(4) responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case (col. 2, lines 30-40; col. 2, line 63-col. 3, line 5).

2. As per **claim 2**, Phelps further discloses the method, wherein the method is performed by computer executable instructions disposed on at least one computer readable medium (figs. 1 and 2; col. 3, lines 60-67).

3. As per **claim 3**, Phelps further discloses the method, wherein the computer executable instructions are distributed among a plurality of hardware platforms (fig. 2; col. 3, lines 60-67).

4. As per **claim 4**, Phelps discloses the method, wherein at least a portion of the computer executable instructions are implemented in a domain specific configuration (fig. 2; "threshold rules").

5. As per **claim 5**, Phelps further discloses the method, wherein at least a portion of the computer executable instructions are implemented in a core infrastructure (fig. 2; col. 1, lines 5-15; col. 2, lines 15-25; col. 3, lines 60-67; "AI pattern recognition system").

6. As per **claim 7**, Phelps further discloses the method, wherein the at least one fraud detection test includes the step of enhancing the network event record such that

an enhanced network event record includes data obtained from at least one external system (fig. 1; col. 4, lines 10-40).

7. As per **claim 8**, Phelps further discloses the method, wherein the enhanced network event record includes data obtained from at least one database (col. 3, lines 60-67).

8. As per **claim 9**, Phelps further discloses the method, wherein the at least one database includes at least one of a configuration database, an event database, a billing database, a call history database, and/or a records database (col. 3, lines 60-67).

9. As per **claim 10**, Phelps further discloses the method, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a threshold rule, the alarm being generated if the network event record violates the threshold rule (col. 5, lines 20-34).

10. As per **claim 11**, Phelps further discloses the method, wherein the alarm is generated if a value in the network event record exceeds a threshold value specified by the threshold rule (col. 5, lines 20-34).

11. As per **claim 12**, Phelps further discloses the method, wherein the alarm is generated if a value in the network event record does not equal a value specified by the threshold rule (col. 5, lines 20-34).

12. As per claim 13, Phelps further discloses the method, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a profile detection rule, the alarm being generated if the network event record violates the profile detection rule (col. 5, lines 20-55).

13. As per **claim 14**, Phelps further discloses the method, wherein the network event record is compared to a normal usage profile (col. 6, lines 1-20).

I 4. As per **claim 15**, Phelps further discloses the method, wherein the network event record is compared to a fraudulent usage profile (col. 5, lines 5-20, 50-58).

15. As per **claim 16**, Phelps further discloses the method, wherein the profile detection rule is based on historical network event records (col. 5, lines 5-50).

16. As per **claim 17**, Phelps further discloses the method, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a predetermined pattern to identify a normal usage and/or a fraudulent usage (col. 6, lines 1-20).

l 7. As per **claim 18**, Phelps further discloses the method, wherein the predetermined pattern is based on call history data (col. 6, lines 1-20).

18. As per **claim 19**, Phelps further discloses the method, wherein the predetermined pattern is generated by a neural network (col. 1, lines 15-20).

19. As per **claim 20**, Phelps further discloses the method, wherein the comparison is performed using tree-based algorithms that generate discrete output values (col. 1, lines 15-20).

20. As per **claim 21**, Phelps further discloses the method, wherein the comparison is performed using statistical based algorithms that that employ iterative numerical processing techniques (col. 1, lines 15-20).

21. As per **claim 22**, Phelps further discloses the method, wherein the step of correlating includes the step of enhancing a network event record by obtaining relevant data from an external source (fig. 2; col. 4, lines 10-40).

22. As per **claim 23**, Phelps further discloses the method, wherein the step of correlating includes the step of applying at least one predetermined fraud analysis rule

to the network event record to decide if a fraud case is appropriate (fig. 2; col. 5, lines 5-55).

23. As per **claim 24**, Phelps further discloses the method, wherein the step of correlating includes the step of applying at least one predetermined prioritization rule to the fraud case to obtain the priority of the fraud case (col. 1, lines 45-60).

24. As per **claim 25**, Phelps further discloses the method, wherein the fraud prevention action may be performed automatically, semi-automatically, or manually based on the priority (fig. 2; col. 5, lines 60-67).

25. As per **claim 26**, Phelps further discloses the method, wherein the fraud prevention action is selected from a group that is comprised of at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification (col. 1, lines 45-60; col. 4, lines 1-10; col. 5, lines 5-20).

26. As per **claim 27**, Phelps further discloses the method, wherein the alarm is selected from a group that is comprised of at least one of a long duration alarm, a call originating alarm, a call terminating alarm, a pin hacking alarm, a simultaneous calls alarm, a geographic alarm, and/or a call interval alarm (col. 5, lines 45-50).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 28-35, and 51-66, are rejected under 35 U.S.C. 103(a) as being unpatentable over Phelps U.S. Patent No. 5,602,906.

27. As per **claim 28**, Phelps discloses a system for monitoring one or more of a plurality of telecommunications networks, each of the plurality of telecommunications networks being characterized by a domain specific implementation, each telecommunications network being configured to generate network event records, each network event record being generated in response to an event occurring in the telecommunications network, the system comprising:

a fraud detection system including a core computing infrastructure and a domain specific infrastructure (AI Pattern recognition), the domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored, the core computing infrastructure (threshold rules) being non-domain specific, the fraud detection system being configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record (fig. 2; col. 2, lines 40-62).

Phelps discloses a fraud detection system including a core computing infrastructure (such as AI pattern recognition analysis system) and domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored (such as a threshold rules see fig. 2) the core computing infrastructure being non-domain specific (col. 1, lines 5-25).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Phelps and incorporate the method wherein a core computing infrastructure and a domain specific infrastructure, the domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored in order to specify the type of computer being used.

28. As per **claim 29**, Phelps further discloses the system, wherein the fraud detection system is dynamically reconfigured to adjust fraud detection rules in accordance with changing patterns of fraud (col. 4, lines 40-50).

29. As per **claim 30**, Phelps further discloses the system, wherein the fraud detection system further comprises:

a detection element coupled to the telecommunication system, the detection element being configured to generate a fraud alarm if the network event record is in violation of a predetermined fraud detection rule (figs. 1 and 2; col. 2, lines 60-67);

an analysis element configured to receive fraud alarms from the detection element, the analysis element being configured to correlate fraud alarms having common aspects, and generate a fraud case based on correlated fraud alarms (col. 5, line 50-col. 6, line 25); and

an expert element coupled to the analysis element, the expert element being configured to apply at least one predetermined expert rule to assign a priority to the fraud case, the expert element performing a fraud prevention action in accordance with the priority (col. 5, line 50-col. 6, line 25).

30. As per **claim 31**, Phelps further discloses the system, wherein the priority is based on a severity of suspected fraud (col. 4, lines 1-10).

31. As per **claim 32**, Phelps further discloses the system, wherein the detection element includes at least one software processing engine comprising computer executable instructions disposed on at least one computer readable medium (figs. 1 and 2; col. 3, lines 60-67).

32. As per **claim 33**, Phelps further discloses the system, wherein the at least one software processing engine is distributed among a plurality of hardware platforms (fig. 2; col. 3, lines 60-67).

33. As per **claim 34**, Phelps discloses a system, wherein the at least one software processing engine implemented in a domain specific configuration (fig. 2; col. 1, lines 5-25)

34. As per **claim 35**, Phelps further discloses the system, wherein the at least one software processing engine includes a rules based thresholding engine configured to read the network event record and compare data in the network event record to a predetermined threshold (col. 2, line 60-col. 3, lines 5; col. 5, lines 20-34).

35. As per **claim 51**, Phelps further discloses the system, wherein the at least one software processing engine in the detection element further comprises:

a profiling database including at least one profile detection rule (col. 1, lines 40-60); and

a protiling engine configured to compare the network event record with at least one profile in accordance with the at least one profile detection rule, the profiling engine generating the alarm if the network event record substantially violates the profile detection rule (fig. 2; col. 1, lines 40-60).

36. As per **claim 52**, Phelps further discloses the system, wherein the profile includes a normal use profile and/or a fraudulent use profile (col. 6, lines 1-25).

37. As per **claim 53**, Phelps further discloses the system, wherein the profile is based on historical network event records (col. 3, lines 25-42).

38. As per **claim 54**, Phelps further discloses the system, wherein the at least one software processing engine in the detection element comprises a pattern recognition engine configured to identify normal and/or fraudulent patterns of usage in the telecommunication network (col. 6, lines 1-25).

39. As per **claim 55**, Phelps further discloses the system, wherein the pattern recognition engine compares the network event record to call history data obtained from a call history database (col. 3, lines 25-40).

40. As per **claim 56**, Phelps further discloses the system, wherein the pattern recognition engine includes a neural network configured to identify fraudulent patterns of usage (col. 1, lines 5-15).

41. As per **claim 54**, Phelps further discloses the system, wherein the pattern recognition engine includes tree-based algorithms (col. 1, lines 5-15).

42. As per **claim 58**, Phelps further discloses the system, wherein the pattern recognition engine includes statistical based algorithms that that employ iterative numerical processing techniques (col. 1, lines 5-15).

43. As per **claim 59**, Phelps further discloses the system, wherein the analysis element further comprises:

an external systems interface component configured to obtain data from external systems relevant to the fraud alarms (fig. 1);

a configuration database configured to specify any additional data required for fraud alarm analysis (col. 3, lines 60-67);

an alarm enhancement component coupled to the external systems interface and the configuration database, the alarm enhancement component being configured to add the additional data and external system data to the fraud alarm (col. 3, lines 60-67); and

a fraud case builder component coupled to the alarm enhancement component, the fraud case builder being configured to correlate and consolidate fraud alarms (col. 5, line 60-col. 6, line 25).

44. As per **claim 60**, Phelps further discloses the system, wherein the fraud case builder is coupled to a rules database, the rules database providing the fraud case builder with parameters for generating fraud cases (fig. 2; col. 3, lines 60-67).

45. As per **claim 61**, Phelps further discloses the system, wherein the expert element further comprises:

a configuration database configured to specify any additional data required for alarm analysis based on an alarm configuration (col. 3, lines 60-67);

an external systems interface component configured to obtain data from external systems relevant to at least one of the alarms (fig. 1);

a prioritizer component coupled to the configuration database and the external systems interface, the prioritizer being configured to direct the external system interface to obtain the additional data from at least one external system based on configuration data obtained from the configuration database, the prioritizer adding the additional data to the fraud case (col. 5, line 60-col. 6, line 25).

46. As per **claim 62**, Phelps further discloses the system, wherein the prioritizer component receives prioritization rules from the configuration database and prioritizes the fraud cases in accordance with the prioritization rules (col. 4, lines 1010).

47. As per **claim 63**, Phelps further discloses the system, wherein the prioritization rules specify the fraud prevention action (col. 5, lines 5-20; col. 6, lines 1-25).

48. As per **claim 64**, Phelps further discloses the system, further comprising an enforcement component coupled to the prioritizer component, the enforcement component performing the fraud prevention action based on the enhanced fraud case (col. 5, lines 5-20; col. 6, lines 1-25).

49. As per **claim 65**, Phelps further discloses the system, wherein the fraud prevention action includes at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification (col. 5, lines 5-20; col. 6, lines 1-25).

50. As per **claim 66**, Phelps further discloses the system, wherein the alarm includes at least one of a long duration alarm, a call originating alarm, a call terminating alarm, a pin hacking alarm, a simultaneous calls alarm, a geographic alarm, and/or a call interval alarm (col. 5, lines 45-50).

Claim 6, and 36-50, are rejected under 35 U.S.C. 103(a) as being unpatentable over Phelps U.S. patent No. 5,602,906 in view of Bowman U.S. Patent No. 5,627,886.

51. As per **claim 6**, Phelps failed to explicitly disclose the method, wherein the at least one fraud detection test includes the step of normalizing the network event record such that the network event record conforms to a predetermined format.

Bowman discloses the method, wherein the at least one fraud detection test includes the step of normalizing the network event record such that the network event record conforms to a predetermined format (col. 7, lines 5-15).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Phelps and incorporate the method wherein the at least one fraud detection test includes the step of normalizing the network event record such that the network event record conforms to a predetermined format as taught by Bowman in order to ensure standard data format.

52. As per **claim 36**, Phelps further discloses the system, wherein the rules based thresholding engine further comprises:

at least one rules database (fig. 2);

a normalizer configured to configured the network event record in a standardized format;

an enhancer component coupled to the normalizer, the enhancer component being configured to insert additional data in the network event record (col. 4, lines 10-40); and

a threshold detector coupled to the enhancer component, the threshold detector being configured to compare the network event record to at least one threshold rule obtained from the at least one rules database, whereby the alarm is generated if the network event record violates the at least one threshold rule (fig. 2; col. 2, lines 60-67).

What Phelps does not teach is a normalizer configured to configured the network event record in a standardized format.

Bowman discloses a normalizer configured to configured the network event record in a standardized format (col. 7, lines 5-15).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Phelps and incorporate the method wherein a normalizer configured to configured the network event record in a standardized format as taught by Bowman in order to ensure standard data format.

53. As per **claim 37**, Phelps further discloses the system, wherein the enhancer component is coupled to an external systems interface, the additional data including data received from an external system (fig. 1).

. 54. As per **claim 38**, Phelps further discloses the system, wherein the network event record includes an event key and at least one feature, the event key identifying the network event and the at least one feature including event measurement data (col. 4, lines 10-30).

55. As per **claim 39**, Phelps further discloses the system, wherein the measurement data includes a count of a number of occurrences of an event during a predetermined time period (col. 4, lines 10-30).

56. As per **claim 40**, Phelps further discloses the system, wherein the measurement data includes a count of a number of like events occurring simultaneously (col. 5, lines 45-50).

57. As per **claim 41**, Phelps further discloses the system, wherein the measurement data includes geographic velocity data (col. 4, lines 50-65).

58. As per **claim 42**, Phelps further discloses the system, wherein the at least one database comprises:

an enhancement rules database coupled to the enhancer component, the enhancer component obtaining an enhancement rule from the enhancement rules database based on data in the network event record (fig. 2; col. 2, lines 40-64; "...including necessary billing information ..."); and

a threshold detection rules database coupled to the threshold detector, the threshold detector obtaining a threshold rule in accordance with data in the network event record (fig. 2; col. 2, lines 40-67).

59. As per **claim 43**, Phelps further discloses the system, wherein the enhancement rule directs the enhancer component to select external data from a selected external source (fig. 1; col. 4, lines 10-40).

60. As per **claim 44**, Phelps further discloses the system of claim 42, wherein the threshold rule stipulates that an alarm is generated when data in the network event record exceeds a threshold value (col. 2, line 60-col. 3, line 5).

61. As per **claim 45**, Phelps further discloses the system, wherein the threshold rule stipulates that an alarm is generated when data in the network event record does not equal a threshold value (col. 2, line 60-col. 3, line 5).

62. As per **claim 46**, Phelps further discloses the system, wherein the enhancer component provides the threshold detector with a feature vector, the feature vector including the event key and a plurality of feature event values, the event key including suspected fraud event identifying data, each feature event value of the plurality of feature event values providing fraud event measurement data (col. 4, lines 10-30).

63. As per **claim 47**, Phelps further discloses the system, wherein the feature event value includes a threshold value (col. 5, lines 20-35).

64. As per **claim 48**, Phelps further discloses the system, wherein the feature vector includes a name field, a value field, and a generating event field for each feature (col. 6, lines 40-60; "call destination").

65. As per **claim 49**, Phelps further discloses the system, wherein the feature vector is implemented as a data structure, the data structure being stored on a computer readable medium (col. 3, lines 60-67).

66. As per **claim 50**, Phelps further discloses the system, wherein the feature vector includes at least one contributing event field for each feature (col. 4, lines 10-30).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on **(571) 272 – 6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington D.C. 20231

Or faxed to:

(571) 273-8300. [Official communications; including After Final communications labeled "Box AF"].

(571) 273-8300. [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"].

Hand delivered responses should be brought to the United States Patent and Trademark Office Customer Service Window:

Randolph Building,

401 Dulany Street

Alexandria VA. 22314

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621
June 13, 2006

PRIMARY EXAMINER